کمپیوٹر سیکیورٹی۔۔۔۔حصہ دوم

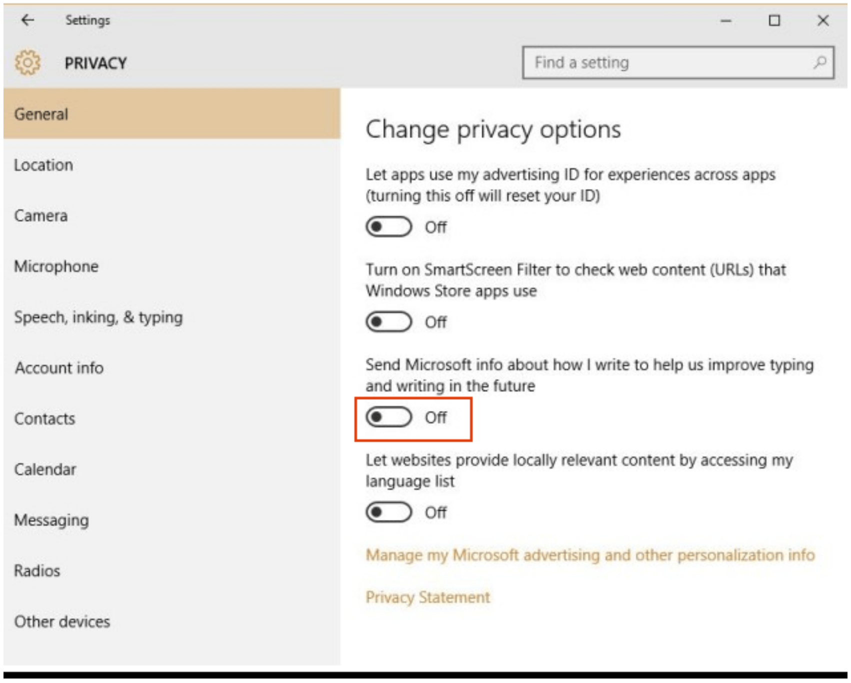
ونڈوز ۱۰ میں پہلے سے انسٹال شدہ کی لاگر کو نکالنے کا طریقہ: ونڈوز ۱۰ میں مائکروسافٹ کی طرف سے پہلے سے ایک کی لاگر انسٹال ہے جو آپ کے تمام لکھائی کی جاسوسی کرتا ہے اور اس کو مائکروسافٹ کی کمپنی پہ بھیجتا ہے۔ اور یہ چھپکے سے نہیں کر رہا، بلکہ اُن کا کہنا ہے کہ اس سے صارفین کو مزید سہولت فراہم کرنا مقصود ہے اور جو اس کو بند کرنا چاہے اسے بند کر سکتا ہے۔ (ہمیں تو کوئی سہولت اس میں دکھائی نہیں دی)۔ خیر اس کو بند کرنے کا طریقہ یہ ہے:

Start پہ کلک کریں، پھر Settings میں جائیں، پھر Privacy میں جائیں

پھر General میں send Microsoft info about how I write... کو Off کریں، جیسا اس تصویر میں دکھایا ہے۔

پھر Speech, inking & typing والے کیٹگری میں جائیں، اور اس میں Stop getting to know me پہ کلک کریں اور ایک اور اسکرین آئی گی اس میں Turn off پہ کلک کریں۔

1



Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

● Off

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use

● Off

Send Microsoft info about how I write to help us improve typing and writing in the future

● Off

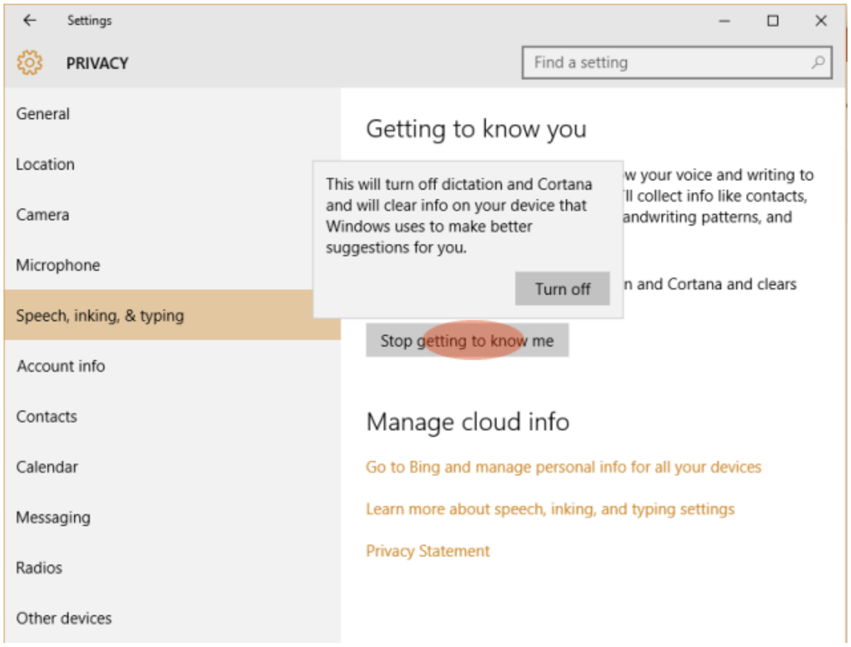
Let websites provide locally relevant content by accessing my language list

● Off

Manage my Microsoft advertising and other personalization info

Privacy Statement

2



Getting to know you

w your voice and writing to 'll collect info like contacts, andwriting patterns, and

n and Cortana and clears

This will turn off dictation and Cortana and will clear info on your device that Windows uses to make better suggestions for you.

Manage cloud info

Go to Bing and manage personal info for all your devices

Learn more about speech, inking, and typing settings

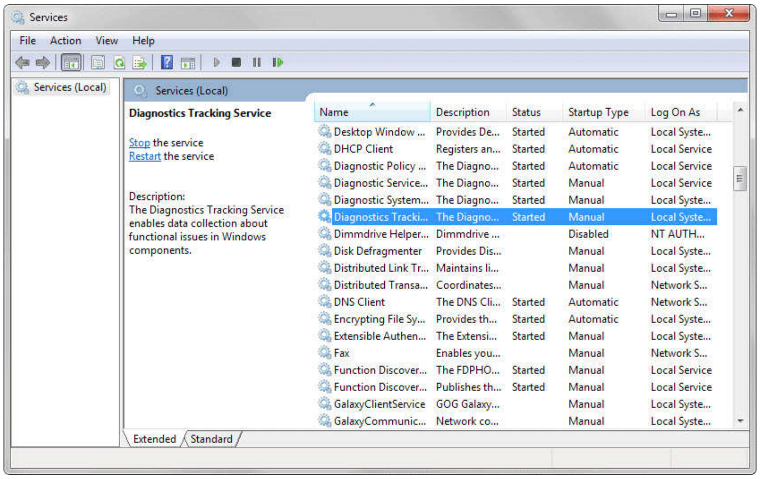
Privacy Statement

اس کے علاوہ آپ کو ایک اور ٹریکنگ آپشن بند کرنا ہو گا، پہلے یہ دیکھیں کی وہ ٹریکنگ آپ کے ونڈوز میں موجود ہے یا نہیں، اس کیلئے ٹاسک مینیجر کو کھولیں، اُس میں Services پہ کلک کریں، پھر سروس میں نیچے ایک آپشن ہو گا Open Services کا اسے کلک کریں،

اب Diagnostics Tracking Service دیکھیں موجود ہے یا نہیں۔۔

اگر موجود ہے تو آپ اس کو یہاں سے stop کر سکتے ہیں۔

مگر یہ دوبارہ اسٹارٹ ہو جاتا ہے، اس لئے اس کو جڑ سے ختم کرنا لازمی ہے



Diagnostics Tracking Service

Stop the service
Restart the service

Description:
The Diagnostics Tracking Service enables data collection about functional issues in Windows components.

Name	Description	Status	Startup Type	Log On As
Desktop Window ...	Provides De...	Started	Automatic	Local Syste...
DHCP Client	Registers an...	Started	Automatic	Local Service
Diagnostic Policy ...	The Diagno...	Started	Automatic	Local Service
Diagnostic Service...	The Diagno...	Started	Manual	Local Service
Diagnostic System...	The Diagno...	Started	Manual	Local Syste...
Diagnostics Tracki...	The Diagno...	Started	Manual	Local Syste...
Dimmdrive Helper...	Dimmdrive ...		Disabled	NT AUTH...
Disk Defragmenter	Provides Dis...		Manual	Local Syste...
Distributed Link Tr...	Maintains li...		Manual	Local Syste...
Distributed Transa...	Coordinates...		Manual	Network S...
DNS Client	The DNS Cli...	Started	Automatic	Network S...
Encrypting File Sy...	Provides th...	Started	Automatic	Local Syste...
Extensible Authen...	The Extensi...	Started	Manual	Local Syste...
Fax	Enables you...		Manual	Network S...
Function Discover...	The FDPHO...	Started	Manual	Local Service
Function Discover...	Publishes th...	Started	Manual	Local Service
GalaxyClientService	GOG Galaxy...		Manual	Local Syste...
GalaxyCommunic...	Network co...		Manual	Local Syste...

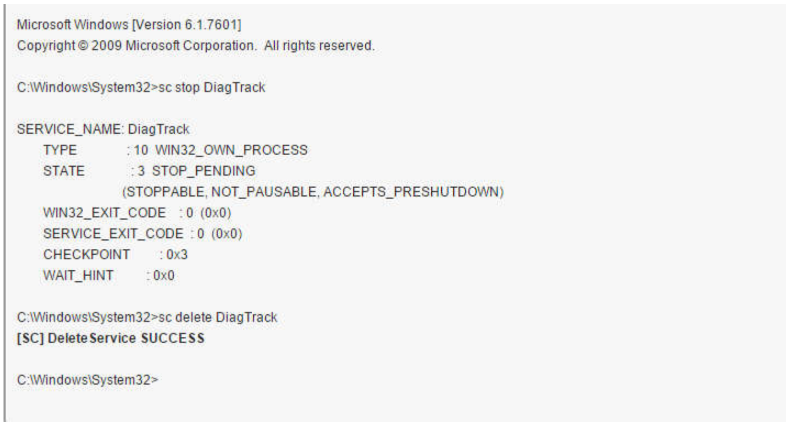
اس کیلئے کمانڈ پرومپٹ/ڈوس/cmd/dos کھولیں۔ ڈوز کھولنے کیلئے سرچ پہ cmd لکھیں command prompt لکھا آئیگا اس کو رائٹ کلک کر کہ Run as administrator سے کھولیں۔ اب اس میں یہ چیز لکھیں

sc stop DiagTrack

انٹر کریں، اس سے وہ بند ہو جائیگا، پھر یہ لکھیں

sc delete DiagTrack

انٹر کریں، اس سے یہ ڈیلیٹ ہو جائیگا۔



```
Microsoft Windows [Version 6.1.7601]
Copyright © 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>sc stop DiagTrack

SERVICE_NAME: DiagTrack
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x0

C:\Windows\System32>sc delete DiagTrack
[SC] DeleteService SUCCESS

C:\Windows\System32>
```

اب اِن سب کو کرنے سے اِن شاءاللہ مائکروسافٹ کے کی لاگر سے محفوظ ہونگے۔

مزید خفیہ رہنے اور انٹرنیٹ کی مکمل ٹریفک کو انکرپٹ اور ٹور کے ذریعے چلانے کیلئے TAILS کا استعمال

مختصر تعارف: TAILS ایک لینگس/Linux آپریٹنگ سیسٹم ہے جس کا مقصد صارفین کی معلومات اور ڈیٹا وغیرہ کو خفیہ رکھنا ہے اور اس کے ذریعے جب آپ انٹرنیٹ استعمال کرینگے تو آپ کی مکمل ٹریفک ٹور/ Tor کے ذریعے چلے گی یعنی انکرپٹڈ ہوگی اور آئی پی ایڈریس بھی تبدیل ہوگی، اس کو آپ ٹور کا آپریٹنگ سیسٹم بھی کہہ سکتے ہیں۔

چونکہ یہ لینکس آپریٹنگ سیسٹم ہے اور جنھوں نے لینکس استعمال نہیں کیا ان کیلئے زیادہ فائدہ مند نہیں ہوگا، بس بنیادی سہولت حاصل کر سکینگے، جو اس میں پہلے سے موجود ہیں اور دیگر سافٹوئیر انسٹال کرنے کیلئے لینکس کا استعمال سیکھنا ہوگا۔ اور جنھوں نے لینکس استعمال کیا ہے اور اس میں تھوڑی بہت مہارت رکھتے ہیں اُن کیلئے انتہائی مفید ثابت ہو سکتی ہے۔ TAILS کو USB میں ڈالنا ہوگا، یعنی TAILS چلانے کیلئے آپ کے پاس کم از کم 4 Gb USB ہونا ضروری ہے۔ یو ایس بی کو بوٹ ایبل بنانا ہوگا جس کا طریقہ آگے بتائینگے۔

TAILS کو یہاں سے ڈاونلوڈ کریں

https://tails.boum.org

اس لنک پہ جاکہ ایک طرف ڈاونلوڈ کا نشان ہوگا، اسے ڈاونلوڈ کریں، تقریباً 1Gb اس کا سائز ہے۔

USB کو بوٹ ایبل/ Bootable بنانے کیلئے آپ یہ سافٹوئیر ڈاونلوڈ کریں

https://rufus.akeo.ie/

اس لنک پہ جائیں اور نیا ورشن ڈاونلوڈ کریں

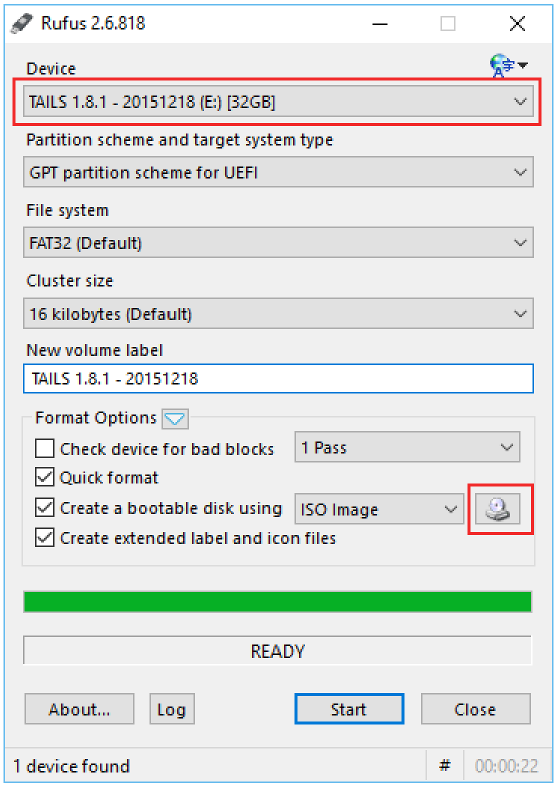
اس کے بعد اب یو ایس بی ڈالیں، اور Rufus سافٹوئیر کو کھولیں۔

اب اس میں Device والے خانے میں اپنے یو ایس بی کا ڈرائیو سیلکٹ کریں۔

پھر نیچے سی ڈی کے نشان پہ کلک کریں جیسا اس تصویر میں دکھایا ہے۔

اس کو کلک کرنے سے ایک ٹیب کھلیگی اس میں TAILS والے فائل کو سیلکٹ کریں، جو آپ نے ڈاونلوڈ کیا تھا۔

اور پھر Start پہ کلک کریں۔ شاید آپ کے ہاں یہ ایرر آجائے۔


Rufus 2.6.818

Device: TAILS 1.8.1 - 20151218 (E:) [32GB]

Partition scheme and target system type: GPT partition scheme for UEFI

File system: FAT32 (Default)

Cluster size: 16 kilobytes (Default)

New volume label: TAILS 1.8.1 - 20151218

Format Options

☐ Check device for bad blocks: 1 Pass

☑ Quick format

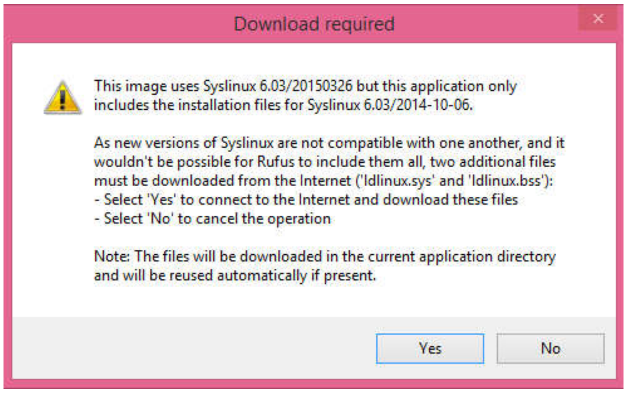
☑ Create a bootable disk using: ISO Image

☑ Create extended label and icon files

READY

1 device found

00:00:22


Download required

This image uses Syslinux 6.03/20150326 but this application only includes the installation files for Syslinux 6.03/2014-10-06.

As new versions of Syslinux are not compatible with one another, and it wouldn't be possible for Rufus to include them all, two additional files must be downloaded from the Internet ('ldlinux.sys' and 'ldlinux.bss'):
- Select 'Yes' to connect to the Internet and download these files
- Select 'No' to cancel the operation

Note: The files will be downloaded in the current application directory and will be reused automatically if present.

اس میں Yes پہ کلک کریں

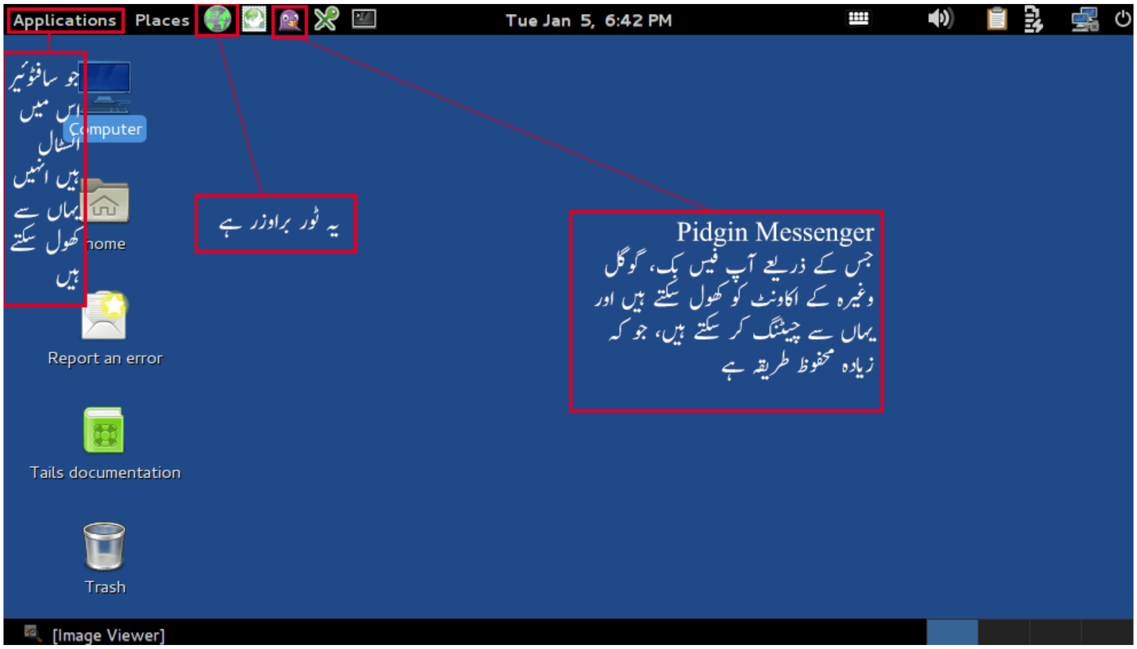
اس کیلئے آپ کو ایک منٹ کیلئے انٹرنیٹ چاہیئے ہوگا کہ ایک ۵۰ کے بی کا فائل ڈاونلوڈ ہوگا۔ پھر فارمیٹ والے آپشن کو Ok کریں۔

بس پھر ایک دو منٹ میں وہ TAILS والی فائل اِس یو ایس میں آجائیگی اور بوٹ ایبل بن جائیگی۔

پھر اس کو چلانے کیلئے اپنے کمپیوٹر کو ری اسٹارٹ کر کہ بائیوز سیٹ اَپ پہ جائیں اور وہاں فرسٹ بوٹ ڈیوائس کو USB کو سیلکٹ کر کہ سیو کریں اور کمپیوٹر ری اسٹارٹ کریں اور پھر اسی TAILS آپریٹنگ سیسٹم سے آپ کا کمپیوٹر اسٹارٹ ہوگا، شروع میں اگر دو آپشن آئیں تو Live والے کو سیلکٹ کریں۔

پھر ایک لاگ اِن کی اسکرین آئیگی اسے لاگ اِن کریں

پھر آپ کا TAILS آپریٹنگ سیسٹم کھل جائیگا، جو اس طرح کا ہوگا



جو سافٹوئیر اس میں انسٹال ہیں انہیں یہاں سے کھول سکتے ہیں

یہ ٹور براوزر ہے

Pidgin Messenger
جس کے ذریعے آپ فیس بک، گوگل وغیرہ کے اکاونٹ کو کھول سکتے ہیں اور یہاں سے چیٹنگ کر سکتے ہیں، جو کہ زیادہ محفوظ طریقہ ہے

ضروری چیزیں تصویر میں لکھ دی ہیں، اس میں بنیادی سافٹوئیر تو پہلے سے انسٹال ہیں مثلاً ویڈیو چلانے کیلئے اور اس طرح کے دوسرے بنیادی سافٹوئیر۔
باقی اس میں ٹیلی گرام اور اس جیسی دیگر ضروری سافٹوئیر انسٹال کرنے کا طریقہ ان شاءاللہ پھر بتائینگے اگر زندگی رہی۔

TAILS کے فوائد:

- اس کو استعمال کرنے سے آپ اپنے ہارڈ سک تک رسائی حاصل نہیں کر سکتے، یعنی جو کچھ یو ایس بی میں ہوگا صرف وہی چیز استعمال کر سکینگے، جس کا فائدہ یہ ہوگا ہیکرز اور حکومت کی جاسوسی سے آپ اور آپ کی فائل محفوظ رہینگی۔
- ہیکرز اور حکومت آپ کی ذاتی معلومات حاصل نہیں کر سکتے یعنی آپ کونسا ڈیوائیس، ونڈوز وغیرہ استعمال کر رہے ہیں اور آپ کی لوکیشن بھی معلوم نہیں کر سکتا۔

- چونکہ ونڈوز میں کافی ایسے سافٹوئیر ہیں جو انٹرنیٹ سے کنیکٹ ہوتے ہیں اور جب آپ آئی پی ایڈریس تبدیل کرتے ہو تو ان کے پاس تو ریکارڈ ہو گا کہ یہ آپ نے ہی استعمال کیا ہے، تو آپ اس خطرے سے بھی محفوظ ہونگے۔
- آپ کی مکمل انٹرنیٹ ٹریفک انکرپٹڈ ہو گی، جس سے دوسروں کو پتا نہیں چلے گا کہ آپ کیا کر رہے ہیں انٹرنیٹ پہ۔
- خاص طور پر اگر آپ کوئی جہادی ویب سائٹ چلا رہے ہیں یا فیس بک پہ کوئی جہادی پیج چلا رہے ہیں اور آپ کو ہیکنگ سے خطرہ ہو تو یہ استعمال کریں۔

نوٹ:

- آپ ہارڈسک تک رسائی حاصل نہیں کر سکتے، اس لئے آپ کو اگر کوئی چیز ضرورت ہو تو آپ ایک اضافی یو ایس بی میں ڈالیں اور اُسی سے استعمال کریں۔
- اس میں جب آپ کوئی سافٹوئیر انسٹال کرینگے یا پھر کوئی فائل ڈاونلوڈ کرینگے وہ صرف اُسی سیشن تک محدود رہیگا اُس کے بعد جب آپ ری اسٹارٹ کرینگے تو وہ ڈیلیٹ ہو جائینگے۔

دیگر چند اہم احتیاطی تدابیر

۱۔ جہادی کاموں کیلئے گوگل، مائکروسافٹ(Hotmail, outlook, live)اور یاہو وغیرہ کے ای میل ایڈریس استعمال نہ کریں۔ کوشش کریں کہ ای میل ایڈریس

https://app.tutanota.de

https://protonmail.com

https://www.hushmail.com

https://safe-mail.net

یہ بنائیں جو بقول اُن کے انکرپٹڈ ہوتے ہیں، اور کوشش کریں کہ ٹوٹونااور پروٹون میل میں ہی بنائیں جو زیادہ معتبر ہیں۔ پروٹون میل میں اکاونٹ بنانے کا طریقہ یہ ہے کہ ایک ریکوسٹ بھیجنا ہوگا جو اسے ۳مہینے کے درمیان میں بن جائیگی۔

۲۔ کسی بھی اجنبی بندے کا میل آجائے اور اس میں کوئی ڈاونلوڈ کی چیز ہو تو اسے ہرگزڈاونلوڈ نہ کریں، جب تک سامنے بندے سے صحیح تعارف نہیں ہوتا۔ اسی طرح کوئی بھی لنک اگر بھیجا ہو وہ بھی نہ کھولیں۔

۳۔ کوشش کریں جس کمپیوٹر سے انٹرنیٹ استعمال کررہے ہیں اس میں ضروری اور خفیہ موادنہ رکھیں، بلکہ ان کو ایسی جگہ رکھیں جہاں انٹرنیٹ استعمال نہیں ہوتا۔

۴۔ کوشش کریں کہ کمپیوٹر میں کم سے کم سافٹوئیر انسٹال کریں۔

۵۔ کبھی بھی ایک نام استعمال نہ کریں بلکہ ہر جگہ دوسرا نام رکھیں، اسی طرح ہر اکاونٹ کا ایک ہی پاس ورڈ نہ رکھیں بلکہ مختلف اکاونٹ کے مختلف پاسورڈ رکھیں اور ان کو وقتاً فوقتاً کو بدلتے رہیں۔

۶۔ جب آپ جہادی ویب سائٹ کھول رہے ہوں یا جہادی مواد دیکھ رہے ہوں تو اس وقت ٹورِنٹ کو بند کیا کریں۔

۷۔ اگر جس کمپیوٹر سے انٹرنیٹ استعمال کررہے ہیں اور اس میں خفیہ مواد بھی موجود ہیں تو اُن کو ایسا نام دیں جو مشکوک نہ ہو یعنی عام سا کوئی نام رکھیں۔

۸۔ ٹیکنالوجی سے اگاہ رہیں، ٹیکنالوجی اور نئی ہیکنگ سے متعلق پڑھتے رہیں۔ ہیکنگ سے متعلق خبریں پڑھنے کیلئے اس ویب سائٹ کو دیکھا کریں

http://thehackernews.com

کسی بھی قسم کا کوئی مشورہ یا معلومات شئیر کرنی ہو تو آپ ہمیں ضرور ای میل کریں۔

اپنے دعاوں میں یاد رکھیئے گا

والسلام علیکم

ای میل ایڈریس:abuturab@tutanota.com

ویب سائٹ:besafer.wordpress.com